Appendix H - Code FIPS User Manual

14870 S Pony Express Rd. #200
Bluffdale, UT 84065
phone: (801) 495-2200 **fax:** (801) 495-0280
web: www.codecorp.com

Specifications subject to change without notice.

© 2011 Code Corporation. All rights reserved.

Code FIPS Overview

The FIPS versions of the Code Reader 2500 FIPS (CR2500 FIPS), Code Reader 3500 FIPS (CR3500 FIPS) and CodeXML® FIPS Bluetooth® Modem (hereafter referred to as the modules) are bar code reading devices that have passed the rigorous testing of the FIPS 140-2 standard. The modules use FIPS approved AES-256 algorithms to encrypt data transmitted wirelessly between the reader and modem.

The versions of the FIPS modules are as follows:

- Code Reader 2500 – 2512FIPS_01 using firmware 4641
- Code Reader 3500 – 3512FIPS_01 using firmware 4641
- CODE FIPS Bluetooth Modem – BTHDFIPS-M2_01 using firmware 0187

The FIPS modules are based on the standard CR2500, CR3500, and CodeXML® Bluetooth® Modem. Therefore most operation questions can be answered in the User Manual for those devices. This document will call out the differences in behavior and operation of the FIPS modules.

Chapter 1 – What you need to know about FIPS Mode

The FIPS modules must be used in a CR2500 FIPS /CodeXML® FIPS Bluetooth® Modem or CR3500 FIPS/CodeXML® FIPS Bluetooth® Modem pair while in FIPS mode. FIPS mode is defined as a reader and modem paired together; transmitting data encrypted with FIPS approved AES algorithms. In order to achieve FIPS mode the reader and modem must be initialized with passwords for two different roles – Cryptographic Officer (CO) and Reader – plus a Key Encryption Key (KEK) that is used to encrypt transmissions of passwords and keys between the reader and modem. The readers and modem come with a default password installed for the CO role. The default password cannot be used to transmit encrypted data and must be updated through the Initialization process. The CO and Reader roles can't be initialized to the same password. Once initialized you may authenticate the CO role or the Reader role by expressly reading a bar code containing the corresponding password. The roles have different purposes and a different set of services that are available to them in the FIPS process, as explained below.

Roles

Cryptographic Officer (CO) – this role can request the following FIPS services:

1. Authenticate to the modules
2. Initialize the modules with new CO and Reader passwords and a new Key Encryption Key (KEK)
3. Zeroization of non-default passwords and KEK

Reader – this role can request the following FIPS services:

1. Authenticate to the modules
2. Transmit encrypted data between the reader and the modem
3. Zeroization of a non-default passwords and KEK

Services

Authentication – This is the service where a role can prove it is authorized to access the modules. Only the CO role can authenticate to the modules using the default password. Either role can authenticate to either module as long as the CO has initialized the modules with new passwords and KEK. Activation of this service is accomplished through reading a Data Matrix bar code that contains the Authentication command plus the password of the role wishing to authenticate.

An Authentication is initiated on the reader. If the Authentication completes successfully on the reader, and the reader is attached to a modem, the Authentication information is transferred to the modem after being encrypted with the KEK. If the Authentication is completed successfully on the modem it returns an acknowledgement to the reader.

Initialization – This is the service that can update the passwords for the roles plus update the KEK on the modules. Only the CO role has access to the Initialization service. Activation of this service is accomplished through reading a Data Matrix bar code that contains the Initialization command plus the new passwords for both roles and a new KEK. An Initialization is initiated on the reader. If the Initialization completes successfully on the reader, and the reader is attached to a modem, the Initialization information is transferred to the modem after being encrypted with the old KEK. If the Initialization is completed successfully on the modem, it returns an acknowledgement to the reader. All subsequent non-data communications between the reader and the modem are encrypted with the new KEK.

Transmitting Encrypted Data – This is the service that transmits data from the reader to the modem using the FIPS approved AES-256 encryption scheme. Only the Reader role has access to this service. Activation of this service is accomplished through completing authentication in the Reader role and reading a bar code containing data. If the transmission is successful the reader will indicate by flashing an LED light amber.

Zeroization – This is the service that removes any customized passwords and KEK from the modules. Either role can access this service at any time. After Zeroization the modules will not return to FIPS mode until the Initialization service has been invoked. Activation of this service is accomplished through reading a Data Matrix bar code that contains the Zeroization command. A Zeroization is initiated on the reader. If the Zeroization completes successfully on the reader, and the reader is attached to a modem, the Zeroization information is transferred to the modem. If the Zeroization is completed successfully on the modem it returns and acknowledgement to the reader.

Critical Security Parameters (CSPs)

The modules utilize four CSPs. They consist of the CO role password, the Reader role password, the KEK and the Traffic Encryption Key (TEK). The passwords and KEK are updated through the Initialization process and the TEK is internally generated by the reader module.

Passwords and keys are made up of hexidecimal characters representing ASCII characters. Hexidecimal values are represented in text by a subscript 'hex' as in $1D_{hex}$. In programming, the passwords and KEK are represented by a leading '%' - %1D.

CO role password – this 64 bit password is used to authenticate the CO role. The modules are shipped with a default CO password of the word 'password' that can only be used to initialize the modules with new CO and Reader role passwords and a new KEK. The modules will not transfer encrypted data using the default password. A 64 bit password is constructed out of eight ASCII characters that can be represented by the hexadecimal digits 20_{hex} through FF_{hex}. Constructing a password to use in the Initialization process is covered below.

Reader role password – this 64 bit password is used to authenticate the Reader role. A 64 bit password is constructed out of eight ASCII characters that can be represented by the hexadecimal digits 20_{hex} through FF_{hex}. Constructing a password to use in the Initialization process is covered below.

Key Encryption Key (KEK) – this 265 bit key is used by an AES algorithm to encrypt transmissions of passwords and keys between the reader and modem modules. A 256 bit password is constructed out of 32 ASCII characters that can be represented by the hexadecimal digits 20_{hex} through FF_{hex}. Constructing a password to use in the Initialization process is covered below.

Traffic Encryption Key (TEK) – this 256 bit key is used by an AES algorithm to encrypt transmissions of data from the reader to the modem. The modem utilizes the same TEK to decrypt the data. The TEK is generated by the reader and is

not accessible by users.

Chapter 2 – Setting up your FIPS hardware

Out of the box the reader/modem pair will behave as any standard non-FIPS pair. You can use them in non-FIPS mode but be aware that any data you transmit will not be protected by the FIPS approved AES-256 encryption algorithms. In order to use FIPS mode the modules must be initialized by the CO. Initialization cannot be performed by the Reader role. You must authenticate the CO role using the default password before Initialization and you must create an Initialization bar code before you can perform Initialization on the FIPS readers.

The reader module provides the interface to the modem module. Therefore, if you wish to Authenticate or Initialize both the reader and the modem you must have the reader paired with the modem while performing these tasks. To connect the reader and modem, read the QuickConnect code printed on the modem with the reader. Refer to the User Manual for the reader and modem for more information on pairing.

Default CO Authentication

The bar code below contains the Authentication command and the default CO password. Using this Authentication the CO can only Initialize or Zeroize the modules.

Figure 1 - Default Cryptographic Officer Authentication Bar Code

Creating an Initialization Bar Code

Create the Initialization bar code by writing a .crb file containing the Initialization commands and data. Convert the .crb file to a Data Matrix bar code by passing it through the CodeXML CRB to Code Utility found at http://codecorp.com/EULACodeXMLCRBtoCodeUtility.php. The Initialization command must be encoded in a Data Matrix bar code in order to function.

The initialization bar code contains six items.

1. The Initialization command (H2; H indicates the FIPS command set, 2 is the Initialization command)
2. A new Cryptographic Officer password (Eight characters in the set 20_{hex} through FF_{hex})
3. A group separator ($1D_{hex}$)
4. A new Reader password (Eight characters in the set 20_{hex} through FF_{hex})
5. A group separator ($1D_{hex}$)
6. A new Key Encryption Key (32 characters in the set 20_{hex} through FF_{hex})

The code below shows example values for the new CO password, Reader password and KEK in a .crb file. You should not use these values when creating an Initialization bar code and the CO and Reader passwords must not be equal. You **must** substitute your own eight character passwords and 32 character KEK when you initialize. The lines starting with ';' are comments. Some comment lines wrap to the next line in this example. Please see your FIPS documentation kit for the actual demo .crb file. The last line that starts with % is the Initialization command. You may omit all comment lines if you wish.

An ASCII to hex converter can be found at http://www.idea2ic.com/PlayWithJavascript/hexToAscii.html. Use the 'De-limit with %' to create hex strings of ASCII characters you can paste into .crb files.

```
;8/6/2010 16:43
```

```
;Initialization command for FIPS Code products


;This example shows
;%48 = H = FIPS Command Set
;%32 = 2 = Initialize Command
;Cryptographic Officer Password is %4E%65%77%50%61%73%73%77 or NewPassw
;Valid Password values are %20 - %FF
;%1D = Group Separator
;Reader Password is %4E%65%77%52%50%61%73%73 or NewRPass
;Valid Password values are %20 - %FF
;%1D = Group Separator

;Traffic Encryption Key is %20%21%22%23%24%25%26%27%28%29%2A%2B%2C%2D%2E%2F%30%31%32%33%34%35%36%37%
38%39%3A%3B%3C%3D%3E%3F or <Space>!"#$%&'()*+,-./0123456789:;<=>?
;Valid Traffic Encryption Key values are %20 - %FF

%48%32%4E%65%77%50%61%73%73%77%1D%4E%65%77%52%50%61%73%73%1D%20%21%22%23%24%25%26%27%28%29%2A%2B%2C
%2D%2E%2F%30%31%32%33%34%35%36%37%38%39%3A%3B%3C%3D%3E%3F
```

The bar code for the above .crb file would look like:

FIPS_Initialization_Example_04

Remember that you can not use the default values to Initialize the FIPS modules and the CO and Reader passwords must not be equal.

Creating a New CO Authentication Bar Code

You must create a new Authentication bar code that contains the new CO password in order to authenticate the CO user after you have initialized the FIPS modules. This is very similar to creating the Initialization bar code. Create a .crb file and process it using CodeXML CRB to Code Utility.

The code below shows the Authentication .crb file that contains a new value for the CO password. This code is provided as an example only and Code Corporation recommends that the password below never be used in your production environment. This is an example based on the CO password 'NewPassw'.

```
; 8/5/2010 20:15
;Authentication command for FIPS Code products

;This example shows
;%48 = H = FIPS Command Set
;%33 = 3 = Authenticate Command

;Cryptographic Officer Password is %4E%65%77%50%61%73%73%77 or NewPassw (Passwords must not contain
%00-%1F)

%48%33%4E%65%77%50%61%73%73%77
```

Creating a New Reader Authentication Bar Code

You must create a new Authentication bar code that contains the new Reader password in order to authenticate the reader user after you have initialized the FIPS modules. This is very similar to creating the CO Authentication bar code. Create a .crb file and process it using CodeXML CRB to Code Utility.

The code below shows the Authentication .crb file that contains a new value for the CO password. This code is provided as an example only and Code Corporation recommends that the password below never be used in your production environment. This is an example based on the Reader password 'NewRPass'.

```
; 8/5/2010 20:15
;Authentication command for FIPS Code products

;This example shows
;%48 = H = FIPS Command Set
;%33 = 3 = Authenticate Command

;Cryptographic Officer Password is %4E%65%77%52%50%61%73%73 or NewRPass (Passwords must not contain
%00-%1F)

%48%33%4E%65%77%52%50%61%73%73
```

Initialization

The Initialization process updates the CO password, the Reader password and the KEK. Now that you have new Authentication, Initialization, and new Authentication bar codes created you can use them to initialize the modules.

Note: Any customization bar codes such as Suffix Enter must be scanned before putting the modules in FIPS mode.

1. Scan the QuickConnect code on the modem to pair the reader and modem modules.
2. Authenticate the CO using the default Authentication bar code (See Figure 1). Observe the indicators on the modules showing that the CO has been authorized. (See section 'FIPS mode indicators on the modules' below)
3. Initialize the modules using the custom Initialization bar code you created above. Observe the indicators on the modules showing that the module has been initialized but no user is authenticated. (See section 'FIPS mode indicators on the modules' below)
4. The FIPS modules are now ready to be authenticated by the Reader role to pass FIPS encrypted data or the CO role to re-initialize again.

Zeroization

The Zeroization process removes the custom passwords and KEK applied in the Initialization process. If the FIPS modules are in an unknown state, Zeroize the modules and re-Initialize. You would also want to Zeroize the modules if you believe the passwords or KEK have been compromised. After Zeroization the modules will respond just as non-FIPS readers and modems until they have been re-Initialized.

Below is the bar code for the Zeroization command:

m765_03

Figure 2 - Zeroization Bar Code

FIPS Mode Indicators On the Modules

Due to the available lights and screens on the different FIPS modules they have slightly different behavior when indicating FIPS modes.

CR2500 FIPS Reader -

The CR2500 module indicates FIPS mode in three stages. The three stages are:

- CO Authenticated – the module will indicate this mode of operation by blinking the blue Left LED light in a 1 second on, 1 second off pattern.
- Un-Authenticated – the module will indicate this mode of operation by blinking the blue Left LED light in a 2 seconds on, 1 second off pattern.
- Reader Authenticated – the module will indicate this mode of operation by blinking the blue Left LED light in a Morse Code 'F' pattern. The Morse Code 'F' is comprised of two short dots, a long dash and a short dot (••−•) followed by a 3.5 second delay.
- Error State – The LED lights will blink (.5 seconds on, .5 seconds off) red to indicate there has been an error in FIPS processing. Clear the error by power cycling the reader by removing and replacing the battery.

CR3500 FIPS Reader -

The CR3500 module indicates FIPS mode in three stages. The three stages are:

- CO Authenticated – the module will automatically indicate this mode of operation by displaying Packet Mode Icon of the letter 'FA' on the top line of the reader display as shown in Figure 3 below.
- Un-Authenticated – the module will automatically indicate this mode of operation by displaying Packet Mode Icon of the letter 'FR' on the top line of the reader display as shown in Figure 4 below.
- Reader Authenticated – the module will automatically indicate this mode of operation by displaying Packet Mode Icon of the letter 'F' on the top line of the reader display as shown in Figure 5 below.
- Error State – The LED light will blink (.5 seconds on, .5 seconds off) red to indicate there has been an error in FIPS processing. Clear the error by power cycling the reader by removing and replacing the battery.

Figure 3 – CR3500 FIPS CO Authenticated Status Indication

Figure 4 – CR3500 FIPS Un-Authenticated Status Indication

Figure 5 – CR3500 FIPS Reader Authenticated Indication

CodeXML® FIPS Bluetooth® Modem

- CO Authenticated – the module will indicate this mode of operation by blinking the LED light in a 1 second on, 1 second off pattern.

- Un-Authenticated – the module will indicate this mode of operation by blinking the LED light in a 2 seconds on, 1 second off pattern.
- Reader Authenticated – The LED light will blink blue in a pattern of a Morse Code 'F' (••—•) onto indicate that the reader is running correctly in FIPS mode.
- Error State – The LED light will blink (.5 seconds on, .5 seconds off) blue to indicate there has been an error in FIPS processing. Clear the error by power cycling the modem by removing and replacing the DIN cable.

Chapter 3 – Using your reader and modem in FIPS mode

Once the modules have been initialized (see above), using them in FIPS mode is straight forward.

1. Scan the QuickConnect code on the modem to pair the reader and modem modules.
2. Read the bar code containing the new Reader password. Observe the indicators on the modules showing that the Reader role has been authenticated. (See section 'FIPS mode indicators on the modules' above)
3. Read bar codes containing data to be sent encrypted by the FIPS approved algorithms.

In the event you believe your module passwords or function has been compromised, scan the Zeroization bar code in Figure 2 above. Caution: Zeroizing the FIPS modules will require a CO to re-initialize the modules to return to FIPS mode.

Chapter 4 – Troubleshooting

- The module is quickly blinking either blue or red
  The module is in an error state. Remove the power by either removing and replacing the battery on the reader or removing and replacing the DIN cable on the modem. These are some of the reasons the modules can error:
  - The CO and Reader passwords match in the Initialization bar code
  - The CO or Reader passwords are not eight characters in the Initialization bar code
  - The KEK is not thirty two characters in the Initialization bar code
  - The reader and modem were initialized with different passwords and then paired
  - There is a corruption in the firmware on the module
  - There is an error in the Self Test the module performs
- The module is indicating 'FR' or blinking 2 seconds on, 1 second off and won't pass data
  The module has been initialized but the Reader role has not been authenticated. Authenticate the Reader role by scanning the new reader authentication bar code created by the CO.
- The modem is indicating that the Reader role has been authenticated, but the reader does not
  The reader has lost its pairing with the modem. Scan the reader authentication bar code and then the QuickConnect code on the modem.
- The module is not indicating FIPS mode
  The module has been Zeroized (the passwords and keys have been removed). Contact your CO to re-initialize the module.